Security Hardening of Implantable Cardioverter Defibrillators

Iram Jaffar
Department of Computer Sciences
Quaid-i-Azam University
Islamabad, Pakistan
ijaffar@ir.qau.edu.pk

Muhammad Usman
Department of Computer Sciences
Quaid-i-Azam University
Islamabad, Pakistan
musman@qau.edu.pk

Alireza Jolfaei
Internet Commerce Security Lab
Federation University Australia
Mt Helen, Australia
a.jolfaei@federation.edu.au

***Abstract*—Contemporary healthcare has witnessed a wide deployment of Implantable Cardioverter Defibrillators (ICDs), which have the capability to be controlled remotely, making them equally accessible from both home and hospitals. The therapeutic benefits of ICDs seem to outweigh potential security concerns, yet overlooking the presence of malicious attacks cannot be justified. This study investigates the scenario where an adversary falsifies a controller command and sends instructions to issue high electric shocks in succession. We propose a novel security hardening mechanism to protect data communications between ICD and controller from malicious data manipulations. Our proposed method verifies the correctness of an external command with respect to the history of heart rhythms. The proposed method is evaluated using real data. Multi-aspect analyses show the effectiveness of the proposed scheme.**

Keywords — Heart defibrillator, implant, security, wireless sensor networks.

I. INTRODUCTION

Over the past decade, the application of Internet of Things (IoT)-enabled consumer electronics devices in the field of e-health has surged tremendously [1], [2]. Nowadays, a wide range of Implantable Medical Devices (IMDs), such as pacemakers, neuro-stimulators and Implantable Cardioverter Defibrillators (ICDs) [3], can provide patients with valuable therapeutic functions in addition to detection, monitoring and recording of patients' vital data [4].

Cardiovascular disease, particularly irregular heart rhythm, is one of the biggest health concerns and it is the leading cause of death for both women and men [5]. ICDs and pacemakers aid in regulating cardiac functions in patients who are at high-risk with life-threatening ventricular arrhythmias. They can also prevent cardiac arrests and sudden cardiac death [6]. These devices are implanted inside the human body and they would normally communicate with an external controller. ICDs transmit patient identification and physiological data, and receive control instructions for operational parameters over unencrypted bidirectional communication channels [7].

Pacemakers and ICDs are energy efficient, resource constrained devices that require an external controller to coordinate their actuations through running computationally expensive data analytics. To this end, an external controller is subscribed to ICDs. The controller aggregates and analyzes the data stream coming from the implants. The controller would use the results of its data mining to make better decisions and actuate certain therapeutic functions to improve the functionality of ICDs. Despite the lifesaving benefits, communications between the controller and the ICD is in plaintext. This leaves ICDs vulnerable to *man-in-the-middle attacks* through which data could be manipulated and this may lead to life-threatening situations. A potential attack can even exploit the transmitter of the controller, which discloses device identification upon probe. This makes it possible for the attacker to replay the controller's command and remain in a position to maliciously maneuver critical parameters in the implanted device, which could be life threatening for the patient.

These devices, in their current form, have very limited or no security mechanisms incorporated [13]. A number of defense methods for wireless insulin pumps have been investigated by Hei and Du [14]. However, cardiac devices vastly remain vulnerable to attacks. Barnaby Jack studied the possibility to command pacemakers to deliver a deadly shock of 830 volts form a laptop in 50 feet vicinity [15]. A group of researchers, in an effort to improve the safety of patients, used a software radio and an oscilloscope to partially reverse engineer the communication protocol of an ICD eliciting that the radio-based attacks, compromising patient safety, could easily be carried out [8].

A recent study [16] has reported unidentifiable communication attempts through wireless medium that trigger the ICD to deliver high-energy shocks in normal heart rhythm. In another study [10], the researchers showed that it is possible to activate the ICD through bypassing current activation procedure, as well as reverse engineer the communication protocol for a long-range channel. For non-emergency scenarios, one of the many solutions that aimed to address the security issues of implantable medical devices (IMDs) was to design security techniques that cut down on energy overheads [17]. Moreover, despite the fundamental importance of IMDs, the software running on these devices remain property of their manufacturers, implying that no attempt to test its security can be made by an independent party [12]. This becomes crucial in the backdrop of proven successful attempts to gain unauthorized access to these devices through software backdoors.

This study investigates the security issues of ICD communication protocol through the lens of man-in-the-middle attacks. In addition, we propose a novel security hardening mechanism to protect data communications between ICD and controller from malicious data manipulations. This study investigates the scenario where an adversary falsifies a controller command and sends instructions to issue high electric shocks in succession. Our proposed method verifies the correctness of an external command with respect to the history of heart rhythms.

The rest of the paper is organized as follows: Section II elaborates the architecture and communication model of ICDs. The ICD network and attack models are detailed in section II. Section III presents specifications and algorithmic description of the proposed method. Formal verification is described in Section IV. The performance of the proposed method is analyzed in Section V. Finally, conclusions are drawn in Section VI.

II. BACKGROUND

ICD constantly monitors heart rhythm and identifies irregular patterns. ICD classifies the category, to which the heart arrhythmia belongs [18]. The classification of heart arrhythmia plays an important role in patient's therapy since irregular heart behaviors, such as Ventricular Fibrillation (VF), require a shock treatment to make the heartbeat normal. Upon detection of a VF, the ICD algorithm puts the capacitor to charge. After the capacitor is charged, the ICD checks to see if VF has subsided or not. If VF is persistent, then ICD delivers a shock. This process is repeated until normal heartbeat is restored. The energy of the shocks delivered is pre-programmed in the algorithm that runs inside the ICD and performs monitoring and therapeutic functions. The level of shock energy is varied depending on the response of the heart to the therapy; it is increased at carefully calculated intervals (usually up to 10 J) or decreased, likewise. To set the upper limit of shock energy that can be delivered to the patient, DFT is calculated and saved in the device after the placement of the implant in human body [19]. Defibrillation Threshold (DFT) is the maximum energy value of therapy for a particular patient with a given heart condition and history.

Fig. 1 depicts the diagram of data communications between an ICD, that is, implanted in a patient, and a controller, that is, inside the healthcare facility. The patient uses a Food and Drug Administration (FDA)-approved portable monitor for self-assessment of their ICDs. This data is sent over the Internet to data servers that make it available to clinicians for further analysis [6]. The medical practitioner uses a controller to remotely monitor, program and actuate the ICD. The controller is equipped with an interface that enables the medical practitioner to input multiple parameters to the ICD through wireless communication [3].

Apart from setting a number of heart-related parameters, the controller is used to deliver one or more shocks to restore normal heartbeat. These shocks are categorized as low-energy (less than 5 J) or high-energy (up to 30 J). High energy shocks have higher probability of being successful [23]. Additionally, the ICDs are programmed to continuously monitor and record heart rate variability, detect arrhythmia, and perform classification into one of the categories such as Atrial Fibrillation (AF), Atrial Tachycardia (AT), Ventricular Tachycardia (VT), and Supraventricular Tachycardia (SVT) amongst many. The focus of this study is on two types of heart conditions at the time when ICD receives an external command:

1) Normal Sinus Rhythm: Fig. 2 (upper panel) shows the condition of EGM when the heart beats normally. In this state, the heart does not require any therapy (shock).

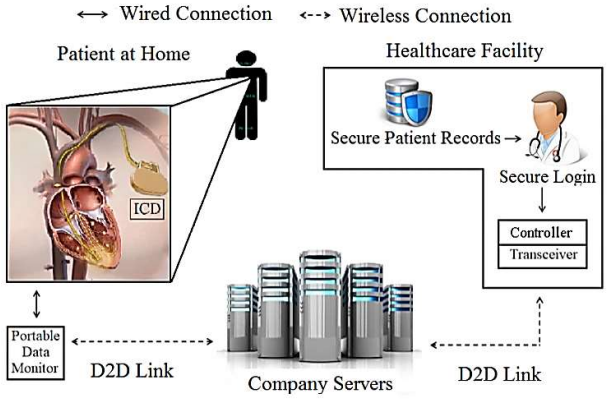

Fig. 1. ICD-controller communication model.

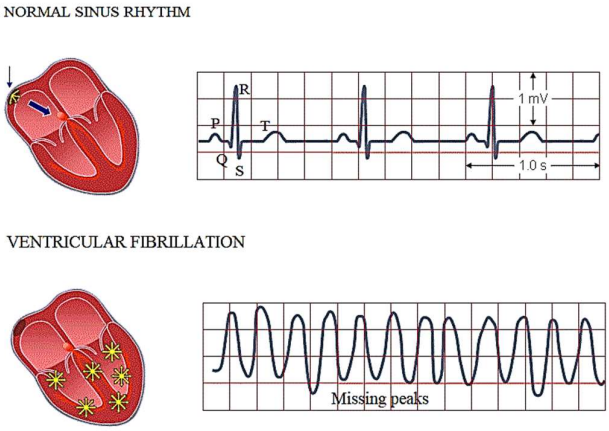

Fig. 2. Upper panel: An EGM of normal heart rate (NSR). Lower panel: EGM of Ventricular Arrhythmia (VF).

TABLE I. NOTATIONS

Notation	Description
DS_t	Device status at given time t
$ECom_t$	External command at time t
$ECom_{t+k}$	External command at time $t+k$
P	Device status: Paused
R	Device status: Running
RS	Device status: Reset (start from beginning)

2) Ventricular Fibrillation: Fig. 2 (lower panel) shows the heart in Ventricular Fibrillation (VF) state. Out of many arrhythmias, this is a critical condition where heart beats 200 times or more per minute and usually requires a shock to restore NSR.

A. Attack Model

TABLE I lists the notations used in this section. As pointed out in [20], the device to device communication between ICD and controller (D2D link) is insecure and vulnerable to data integrity attacks [21]. In the following, we discuss a '*blind therapy override*' attack scenario.

The ICD receives an antagonist command, instructing the device to pause the routine algorithm execution and issues one or more high-energy shocks in succession to the patient. This external command (ECom) does not comply

with the current heart condition, which is a primary factor in determining the basis for the shock(s) to be delivered. The ICD capacitor can deliver multiple shocks with the same charge. ECom is defined as

$$\text{ECom}_t = \bigcup_{p=1}^{r} ED_p, \quad (1)$$

where *ED* denotes the high energy shock(s) to be delivered and *p* is a variable which denotes the instances that may vary from 1 to *r*. *ED* is defined as a function of capacitance *Ca* and shock waveform voltage *V* as follows [18]:

$$ED_p = \frac{1}{2} Ca_p V_p^2. \quad (2)$$

At a given time *t,* ECom is programmed to deliver all shocks in succession. Each shock instance is capable of charging the capacitor for these 'blind' therapies. The shocks are termed as blind, because they execute blindly, without taking into account the current heart condition, thus posing a fatal attack.

III. Proposed Security Hardening Method

In this section, we propose an integrity protection mechanism that can mitigate the attack scenarios explained in Section II. This mechanism complements the existing algorithm working inside the ICD. Our proposed mechanism adds security features in the functionality of ICD and is suitable for the resource-constrained microcontrollers used in the implanted device. The status number of ICDs can be used to detect malicious interruptions/commands, because the status number would pause in the presence of external interruptions/commands. When an intrusion is detected, a flag is set to 1. This will show the type of access that the external command seeks, that is, capacitor access (flag = 1). A variable *access type* is used to store this value.

Let *m* denote memory cells, where physiological data are stored and *i* denote the index of *m.* For *r* number of available memory locations, memory *M* and index *I* are defined as $M = \{m_1, m_2, ..., m_r\}$ and $I = \{i_1, i_2, ..., i_r\}$. We assume that $i_g, i_h, i_l \in I$ are indexes for locations $m_g, m_h, m_l \in M$ that store the values of the current heart condition, the dynamically calculated DFT, and E' (Equation (5)), respectively. The algorithm uses three memory pointers **p*, **q and *r* to point to memory locations m_g, m_h, and m_l, respectively.

The variable *access type* with value *Therapy* first saves the incoming shock strength into a variable Th_{ss}, which is later used to compare against DFT (upper shock limit set for the device). The statement following the pointers makes a comparison **p = NSR*. If this holds true, it implies the heart is functioning normally and no therapy is required. However, if the heart condition is VF, then it is a confirmed case for therapy. In this case, a safety zone (SZ_{ECom}) is computed. The safety zone has two limits: an upper limit and a lower limit. The value of Th_{ss} is checked with respect to these limits so that ICD would be able to assess the safety of the external energy level for therapy. SZ_{ECom} is defined as

$$E' \leq Th_{ss} \leq DFT_{dyn}, \quad (3)$$

where

$$DFT_{dyn} = E' + \bar{s} + 10, \quad (4)$$

and

$$E' = \lceil \sum_{i=1}^{n} \bar{E}_{VF_i} / n \rceil, \quad (5)$$

where

$$\bar{E} = \sum_{d=1}^{w} E_d / Tcount. \quad (6)$$

The notation $\bar{E}$ in Equation (6) is the expected value of energy delivered E_d per episode of VF. If *w* is assumed to be the different number of times the therapy is administered for each episode of VF, *Tcount* stores this value.

The value of E' in Equation (5) gives us the upper limit of any fraction obtained through computing average for a sample of *n*, since the safety zone should contain close and strict boundaries for providing maximum safety and most efficient therapy results.

The notation *s* in Equation (7) is the standard deviation of the values of energy delivered ranging from 1 to *w* for each episode of VF. $\bar{E}$, being the average of the cumulative energy per episode, gets subtracted from each value of energy delivered and squared. The sum of all such values divided by *n*-1 gives the standard deviation for *Tcount* number of therapies per episode of VF.

$$s = \sqrt{\frac{\sum_{d=1}^{w} \left(E_{VF_d} - \bar{E}\right)^2}{\text{n}-1}}, \quad (7)$$

$$\bar{s} = \lceil \sum_{i=1}^{n} s/n \rceil, \quad (8)$$

where $\bar{s}$ is the ceiling of the average of *n* values of *s* for a sample of *n* VF episodes. Again, the ceiling is acquired to obtain the upper limit of energy. DFT dynamic, DFT_{dyn} is the value of standard deviation $\bar{s}$ added to E' to get the upper limit or the maximum energy that defibrillates successfully. An additional energy of 10 J in Defibrillation Threshold is set as the value of the upper limit of shock energy that can be used for setting shock parameters in an attempt to restore heart function to NSR in minimal number of attempts [20].

A variable *BurstCount* is used to keep track of how many times therapy is administered for a single episode of VF. For each shock initiated, *BurstCount* gets incremented by one. It is then compared with x' which is defined as the floor of $\bar{x}$.

$$x' = \lfloor \bar{x} \rfloor, \quad (9)$$

where $\bar{x} = \sum_{b=1}^{n} VF_{bTcount} / n$.

The notation $\bar{x}$ is the average of single values of *Tcount* for our sample of *n* VF episodes. The reason for flooring $\bar{x}$ is to keep the total number of therapies administered to a minimum, given that only high-energy shocks are under consideration. If *BurstCount* exceeds the average value of number of therapies, the shock is aborted.

Next, if the value of the shock strength from the external command is found to be greater than the upper safe limit, only a single shock equal to the strength of upper limit will be initiated. The algorithm also performs a classification of resultant heart condition after the first shock has been administered. This is a requirement in order to get an updated heart condition.

For all successive therapy commands, these conditions are checked repeatedly until the heart condition is found normal (NSR). This also helps to rule out the possibility of invalidating a command issued from an authentic source taking care of an emergency scenario. Algorithm 1

summarizes the functionality of detection of an external command and classification procedure.

Algorithm 1: Detection of an external command and its classification

Input: $ECom_t$
Output: Therapy or Warning
Initialization: SZ_{ECom} = False; BurstCount = 0
1: $DS_t \leftarrow P$; //external command detected
2: if Flag = 1 then
3: AccessType ← Therapy;
4: if AccessType = Therapy then
5: $Th_{ss} \leftarrow$ measure(ECom.ShockStrength);
6: *p ← fetch(i_g); //fetch current heart condition
7: *q ← fetch(i_h); //fetch upper limit of safety zone
8: *r ← fetch(i_l); //fetch lower limit of safety zone
9: if *p = NSR then //if heart is normal
10: AbortTherapy();
11: goto 27;
12: else if *p = VF then
13: *Compute* SZ_{ECom} ; //boolean variable
14: if SZ_{ECom} then //the energy is in safe range
15: DeliverTherapy();
16: Increment BurstCount; //additional check
17: $m_g \leftarrow$*Classify resultant heart condition*;
18: if BurstCount ≤ x'
19: goto 5;
20: else //if BurstCount has exceeded average
21: AbortTherapy();
22: IssueWarning();
23: goto 27;
24: else if $Th_{ss} > DFT_{dyn}$ then
25: $Th_{ss} \leftarrow DFT_{dyn}$;
26: goto 15;
27: $DS_t \leftarrow RS$;

IV. FORMAL VERIFICATION

We use formal verification for our proposed algorithm in order to verify its correctness. A finite state model of the proposed system is presented in Fig. 3. The model is used to identify two types of requirements: *Safety* and *Liveness* [22]. Safety requirement refers to the behavior of the system that must not happen; whereby, liveness requirement means a system behavior that will eventually happen.

Our proposed algorithm comprises three states: *Classify, Shock* and *Warning.* These states are inter-reachable through transition arrows. The numbers on the arrows represent the respective Linear Temporal Logic (LTL) requirement as explained in Table II. The proposed algorithm has been tested for safety and liveness requirements using NuSMV verification tool. NuSMV formally verifies LTL properties of a given system [23].

First, the LTL requirements of our proposed algorithm were laid out. Next, NuSMV was fed with each requirement and resultant verdict from the model checker was obtained. For each LTL requirement, our algorithm obtained a *pass* verdict, which implies that all requirements stand formally verified. Table II presents the LTL requirements for our proposed algorithm. The occurrence of ECom is a pre-condition for the state model of the proposed algorithm. In other words, when the ICD receives an external command, the primary algorithm gets paused; these five requirements are checked for safety or liveness before any of the shocks programmed in ECom are initiated. The output of *classify* is internally used as an input for the states of *Shock* and *Warning*.

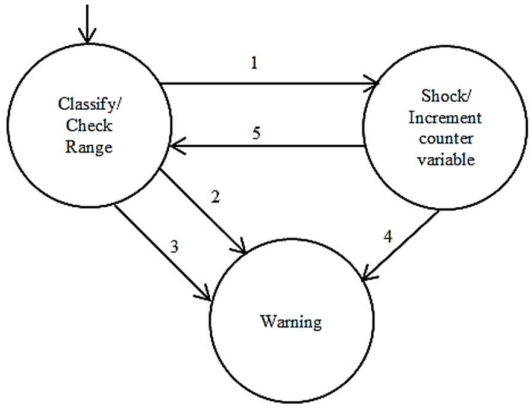

Fig. 3. Finite state model of the proposed algorithm.

TABLE II. LTL REQUIREMENTS

Transition	LTL Requirement	Type	Output
1	Check: VF state active AND number of shocks delivered are less than or equal to counter variable (Burstcount) AND shock strength in ECom is within the safety range	Liveness	Shock
2	Check: Normal heartbeat	Safety	Warning
3	Check: Shock strength in ECom is outside safety range	Safety	Warning
4	Check: The number of shocks delivered is greater than counter variable	Safety	Warning
5	Check: The number of shocks delivered is less than or equal to counter variable	Liveness	Classify

V. PERFORMANCE ANALYSIS

To analyze the performance of the proposed algorithm, the surrogate values of energy allegedly entered by an adversary at the interface of a simulated controller are randomly generated. These values are then used to ascertain if a shock of a certain energy level is sufficient to defibrillate successfully. This can turn malicious attempts into defibrillation therapies.

The average number of therapies required for each of the 16 episodes of VF is assumed randomly as 3, 1, 2, 3, 2, 1, 2, 3, 3, 2, 2, 1, 1, 2, 3, 2. These values span a range between 1 and 3, depicting the usual number of therapies required, on average, by the ICD to successfully defibrillate [24]. The average energy value for each episode is assumed randomly between 18 and 40. This range specifies the most common values of energy (in joules) used by ICD for therapies [18]. The values are taken as 25, 28, 20, 32, 22, 18, 23, 30, 40, 25, 21, 19, 30, 25, 26, 35. The calculations for the sample mean are performed on these values. Further, statistical computations are made on the basis of values obtained from the first step.

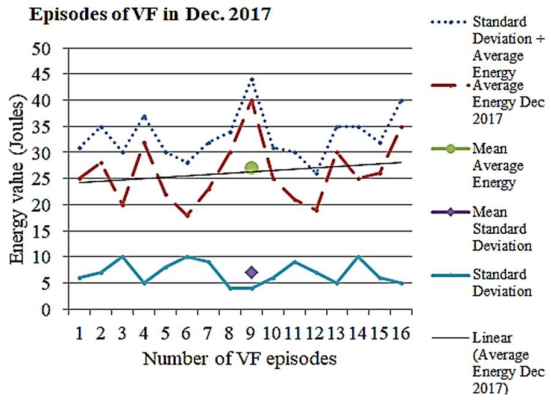

Fig. 4. Anatomy of DFT Dynamic and lower threshold of shock energy.

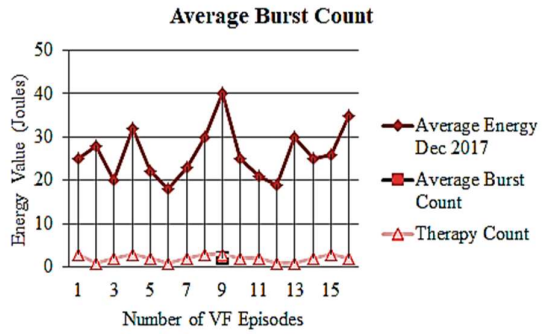

Fig. 5. Average number of therapies administered for a sample of 16 episodes of VF.

Fig. 4 plots the average energy of the total number of shocks administered per episode of VF for Patient A. A total of sixteen episodes of VF are taken for the month of December 2017. It becomes obvious through this pictorial representation that using an upper threshold of energy might not be safe, as its value exceeds the maximum energy for the entire range of values under examination. The proposed algorithm uses the *mean* of average energy values added in the mean of *standard deviation* computed previously for each value to ascertain dynamic DFT (that is, the safe upper threshold).

In the following, Cases 1 and 2 elucidate how the proposed algorithm caters varying values of shock strength in *ECom*, whereas Case 3 examines how an additional check curtails a string of successive shocks.

Case 1. External shock strength lies within safety zone: Consider, for example, a scenario where the ICD detects an external command with the instruction to administer a shock of 40 J (890 Volt) [5]. For computing safety zone, assume that the proposed algorithm is currently using the December 2017 window, where the sample size n =16 (total number of VF episodes in the month). Against each episode, the average energy value is used to compute mean (ceiling) of n episodes: E' = 27. A single value of $\bar{E}_{VFi}$ is the mean of total energy required for the specific number of shocks to restore NSR for one episode of VF. Next, the standard deviation computed for each episode is used to compute the mean standard deviation (ceiling) for n values. $\bar{s}$ = 7. The upper limit of the safety zone is now computed by adding 10 J to E' plus $\bar{s}$, refer to Equation (4), which gives the value of 44 as DFT_{dyn}. The proposed algorithm now compares the shock strength of the first shock instruction of ECom with 44. Since 40J < 44J, the proposed algorithm establishes that the shock strength of external command lies below the maximum shock energy threshold for Patient A, and thus initiates the shock.

Case 2. External shock strength exceeds upper threshold of safety zone: Assume that the shock strength of the external command is 55 J and the heart condition as classified by the primary algorithm is VF. A defibrillation shock remains a requirement. The algorithm, upon entering Statement 25, assigns the value of DFT_{dyn} to Th_{ss}. Thus, the maximum energy shock that can be administered is equal to the upper bound of the safety zone. Since there is no study so far, to the best of our knowledge, that gives a comparison between incremental (mostly used by primary algorithm of ICD) and high-energy (override through programmer) shocks, the possibility of deploying shock commands in override mode have a higher probability of providing successful defibrillation, in addition to letting the additional charge time allow termination of non-sustained arrhythmic conditions [24].

Case 3. Curtailing the number of shocks to *BurstCount*: Consider that an external command is detected with a series of shocks to be administered, assuming the shock energy of each falls under the maximum limit of 44 J, allowing the proposed algorithm to initiate therapy. After each therapy, the proposed algorithm increments a counter variable *BurstCount* which is initialized to 0 and compares that with pre-computed x' = 2. Fig. 5 elaborates how the value of x' is computed for a window of n values. Hence, after two instances of therapies, the comparison will result in a False, and further therapy will be aborted with a warning beep.

A. Overheads Analysis

Time complexity. The proposed algorithm costs a constant time factor for its variable assignments, comparisons, and computation of statistical parameters. However, the time complexity of the comparison statement of BurstCount with x' is $O(k \cdot n)$, where k is a constant such that $0 < k \leq 1$. If the value of pre-computed x' equals the number of therapies in the external command, the worst-case time complexity of the algorithm becomes $O(n)$. To save the time complexity, the lower/upper bounds of the safety range (equations (4) and (5)) can be precomputed and stored in the ICD microcontroller.

Space overheads. Ignoring the single bit requirement of the Boolean type variable Flag, the three pointers cost 4 bytes each, and the variable BurstCount of integer type costs 1 byte. Hence, the total approximate space overhead is 13 bytes, which is a fraction of the typically available 128 KB of memory [8].

Energy consumption. Each notification beep of the ICD costs negligible voltage of the lithium battery. The proposed algorithm initiates only one warning beep and proposes beep accompanying vibration for up to 3 seconds, which is half

the duration of most standard delivery vibrations. Also, the number of notifications for a single event is proposed to be curtailed to at most two recursions, thereby not posing a resource hungry constraint.

VI. Conclusion

This study proposes a novel scheme to enhance safety and security of ICDs. To mitigate the adversarial attacks, the proposed method employs a fail-safe logic, which is incorporated as a part of the source code within ICDs. This method was devised to counter an attack that could potentially endanger the patient's life. To mitigate this attack, our proposed algorithm uses the latest window of patient data to compute the required upper threshold of shock energy that can successfully defibrillate. The upper threshold is then used as a sanity check to detect and weed out high-energy shocks initiated by adversaries. Additionally, the algorithm is capable of converting life-threatening commands to defibrillation therapies by limiting the energy to the upper threshold. For a third counter-measure, our scheme uses a recent history of patient data to keep a track of the number of times therapy is required for each episode of VF. This counter is used as a check to compare how many times the external command has successfully initiated the shock, and hence, maintains patient's safety.

References

[1] J. Bai, S. Lian, Z. Liu, K. Wang, and D. Liu, "Smart guiding glasses for visually impaired people in indoor environment," *IEEE Transactions on Consumer Electronics*, vol. 63, no. 3, pp. 258-266, August 2017.

[2] G.K. Garge, C. Balakrishna, and S.K. Datta, "Consumer Health Care: Current Trends in Consumer Health Monitoring," *IEEE Consumer Electronics Magazine*, vol. 7, no. 1, pp. 38-46, December 2017.

[3] D. Halperin, T.S. Heydt-Benjamin, B. Ransford, S.S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno, and W.H. Maisel, "Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses," in *Proc. IEEE Symposium on Security and Privacy*. Oakland, California USA, May 2008, pp. 129-142.

[4] G. Zheng, R. Shankaran, M.A. Orgun, L. Qiao, and K. Saleem, "Ideas and Challenges for Securing Wireless Implantable Medical Devices: A Review," *IEEE Sensors Journal*, vol. 17, no. 3, pp. 562-576, December 2016.

[5] U.R. Acharya, H. Fujita, M. Adam, O.S. Lih, V. K. Sudarshan, T.J. Hong, J.E. Koh, Y. Hagiwara, C.K. Chua, C.K. Poo, and T.R. San, "Automated characterization and classification of coronary artery disease and myocardial infarction by decomposition of ECG signals: A comparative study," *Information Sciences*, vol. 377, pp. 17-29, January 2017.

[6] A. Müller, T.M. Helms, H. Wildau, J.O. Schwab, and C. Zugck, "Remote Monitoring in Patients with Pacemakers and Implantable Cardioverter-Defibrillators: New Perspectives for Complex Therapeutic Management," *Modern Pacemakers - Present and Future*, Mithilesh R. Das (Ed.), InTech, 2011, pp.147-166.

[7] F.B. Ransford, S.S. Clark, D.F. Kune, K. Fu, and W.P. Burleson, "Design Challenges for Secure Implantable Medical Devices," *Security and Privacy for Implantable Medical Devices*, Wayne Burleson (Ed.), Springer, New York, USA, pp. 157-17, September 2013.

[8] D. Halperin, T.S. Heydt-Benjamin, K. Fu, T. Kohno, and W.H. Maisel, "Security and Privacy for Implantable Medical Devices," *IEEE Pervasive Computing*, vol. 7, no. 1, pp. 30-39, January-March 2008.

[9] X. Zhu, M. Noro, and K. Sugi, "Computer simulation of defibrillations using subcutaneous implantable cardioverter-defibrillators," in *Proc. IEEE 6th International Conference on Awareness Science and Technology*, Paris, France, pp. 1-6, 2014.

[10] N. Ellouze, M. Allouche, H.B. Ahmed, S. Rekhis, and N. Boudriga, "Securing implantable cardiac medical devices: use of radio frequency energy harvesting," In *Proc. 3rd ACM International Workshop on Trustworthy Embedded Devices*, Berlin Germay, November 2013, pp. 35-42.

[11] G. Zheng, R. Shankaran, M.A. Orgun, L. Qiao, and K. Saleem, "Ideas and Challenges for Securing Wireless Implantable Medical Devices: A Review," *IEEE Sensors Journal*, vol. 17, no. 3, pp. 562-576, February 2017.

[12] L. Wu, X. Du, M. Guizani, and A. Mohamed, "Access Control Schemes for Implantable Medical Devices: A Survey," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1272-1283, October 2017.

[13] E. Marin, D. Singelée, F.D. Garcia, T. Chothia, R. Willems, and B. Preneel, "On the (in)security of the latest generation implantable cardiac defibrillators and how to secure them," In *Proc. 32nd Annual Conference on Computer Security Applications*, ACM, New York, NY, USA, pp. 226-236, December 2016.

[14] X. Hei, and X. Du, "Conclusion and Future Directions: Defending Scheme Set," In *Emerging security issues in wireless implantable medical devices*, Xuemin Shen (Ed.), Springer, New York, USA, pp. 45-47, January 2013.

[15] C. Camara, P. Peris-Lopez, and J.E. Tapiador, "Security and privacy issues in implantable medical devices: A comprehensive survey," *Journal of Biomedical Informatics*, vol. 55, pp. 272-289, June 2015.

[16] M. Assaad, G. Degheim, and C. Machado, "The runaway defibrillator…A case of an implantable cardioverter-defibrillator that failed communication and deactivation with a magnet," *Heart Rhythm Case Reports*, Volume 2, Issue 1, pp. 40–42, 2016.

[17] S. Hosseini-Khayat, "A lightweight security protocol for ultra-low power ASIC implementation for wireless Implantable Medical Devices," *In Proc. 5th International Symposium on Medical Information and Communication Technology*, Montreux Switzerland, pp. 6-9, May 2011.

[18] M.R. Gold and C. Swerdlow, "The implantable cardioverter-defibrillator" in *Cardiac Pacing and ICDs,* K.A. Ellenbogen and K. Kaszala (Eds.), *6*th ed. West Sussex, UK: John Wiley & Sons. Ltd., pp. 323-373, March 2014.

[19] M. Madhavan and P.A. Friedman, "Optimal Programming of Implantable Cardiac-Defibrillators," *American Heart Association,* vol. 12, no. 6, pp. 659-672, 2013.

[20] S. Challa, M. Wazid, A.K. Das, and M.K. Khan, "Authentication Protocols for Implantable Medical Devices: Taxonomy, Analysis and Future Directions," *IEEE Consumer Electronics Magazine*, vol. 7, no. 1, pp. 57-65, January 2018.

[21] A. Jolfaei and K. Kant, "A lightweight integrity protection scheme for low latency smart grid applications," *Computers and Security*, 2018.

[22] M. Usman, V. Muthukkumarasamy, and X.-W. Wu, "Specifications and Validation of Agent-based Anomaly Detection and Verification System for Resource Constrained Networks," *Journal of Networks*, July 2015.

[23] P. Arcaini, A. Gargantini, and E. Riccobene, "NuSeen: A Tool Framework for the NuSMV Model Checker," *IEEE International Conference on Software Testing, Verification and Validation (ICST)*, Tokyo, 2017, pp. 476-483.

[24] F. Mansour and P. Khairy, "ICD follow-up and troubleshooting," in *Cardiac Pacing and ICDs,* K.A. Ellenbogen, and K. Kaszala (Eds.), *6*th ed. West Sussex, UK: John Wiley & Sons. Ltd., pp. 413-452, March 2014.